CLAIMS

What is claimed is:

Sub a1

1. A method for generating a key pair, the method comprising:

- forming a private key which includes at least one enhancing key; and
- forming a public key which includes a commitment to said at least one enhancing key, wherein the public key and the private key form the key pair.

2. The method as recited in Claim 1, wherein the step of forming a public key comprises computing a function on a commitment to an enhancing key and a 1-time public key.

3. The method as recited in Claim 1, wherein the enhancing key is randomly chosen.

4. The method as recited in Claim 1, further comprising employing the enhancing key in a process.

5. A method as recited as in Claim 4, wherein the process performs a hash calculation.

6. A method as recited in Claim 1, further comprising computing a certificate for the public key.

7. A method as recited as in Claim 1, wherein the commitment is a TCR commitment.

8. The method as recited in Claim 7, further comprising employing the enhancing key in a process.

9. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for generating a key pair, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 1.

10. A method of forming a TCR commitment comprising:
- providing a commitment for a first string, and
- applying a TCR function to a second string that includes the commitment.

11. A method as recited in Claim 10, wherein the step of applying includes:
- choosing a random key for the TCR function.
- evaluating the TCR function on the random key and the second string.

12. A method as recited in Claim 11, wherein the TCR function is a basic cryptographic primitive.

13. A method as recited in Claim 12, wherein the cryptographic primitive is the SHA-1 compress function.

14. A method as recited in Claim 10, wherein the step of applying forms a TCR function output which is 80 bits long.

15. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a key pair, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

16. A method as recited in Claim 10, further comprising employing the TCR commitment in an enhanced commitment based signature scheme.

17. A method as recited in Claim 1, wherein the public-private key pair is used a bounded number of times.

18. A method as recited in Claim 17, where the bounded number is 36.

19. A method as recited in Claim 12, wherein the TCR function is a TCR hash tree based on a basic cryptographic primitive.

20. A method as recited in Claim 1, further comprising employing the key pair in a commitment based signature scheme.

21. The method as recited in Claim 4, wherein the process is a 36-time signature scheme.

22. A method as recited in Claim 10, further comprising employing the TCR commitment in an E-commerce protocol.

23. A method comprising:

generating a TCR committment opening function for extracting a data string committed to by at least one TCR commitment message,

utilizing a corresponding TCR opening string for each said at least one TCR commitment message, and

employing a TCR function and a regular commitment scheme used in generating said at least one TCR commitment message and used in generating said corresponding TCR opening string.

24. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR committment opening function for extracting a data string committed to by at least one TCR commitment message,, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 23.

25. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing generation of a TCR committment opening function, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the steps of claim 23.

26. A method as recited in Claim 25, wherein the step of generating the TCR commitment function includes:

receiving a data string to be committed and receiving secret information if any in said regular commitment scheme;

computing a regular commitment message using said regular commitment scheme upon both said data string and said secret information;

randomly selecting a key for said TCR function;

computing said TCR function on said key and said regular committment message and obtaining a resulting hash value;

forming a TCR commitment message including said resulting hash value and said key, said TCR commitment message being an output of said TCR commitment function.

27. A method as recited in Claim 26, further comprising saving said regular commitment message.

28. A method as recited in Claim 27, wherein the step of saving is performed for a commiter.

29. A method comprising:

generating a TCR de-commitment function for de-committing at least one TCR commitment message employing a TCR function and a regular commitment scheme used in generating said at least one TCR commitment message.

30. A method as recited in Claim 29, wherein the step of generating the TCR de-commitment function includes:

receiving a data string committed and receiving secret information used in generating said at least one TCR commitment message if any;

receiving a regular commitment message computed as part of generation of said at least one TCR commitment message;

computing the regular de-commitment function on using said regular commitment message, said data string and said secret information and generating a regular opening string;

forming a TCR opening string including said regular opening string and said regular commitment message, said TCR opening string being an output of said TCR de-commitment function.

31. A method comprising:

generating a TCR commitment function by employing any TCR function and utilizing any regular commitment scheme.

32. A method as recited in Claim 23, wherein the step of generating the TCR commitment opening function includes:

receiving a TCR committment message and a corresponding TCR opening string;

extracting a hash value and a key from said TCR committment message; and

extracting a regular opening string and a regular commitment message from said corresponding TCR opening string

computing the TCR hash function with said key and said regular committment message forming a result value; and

comparing said result value with said hash value.

33. A method as recited in Claim 32, further comprising reporting an error if the step of comparing results in a non-compare, and reporting a non-error if the step of comparing results in a compare.

34. A method as recited in Claim 32, if the step of comparing results in a compare, further comprising applying said regular opening commitment function on said regular opening string and said regular commitment message to produce said data string,.

35. A method comprising:

constructing a TCR commitment scheme comprising:

a TCR commitment function;
a TCR de-commitment function; and
a TCR committment opening function,

by employing any TCR function and any regular commitment scheme.

36. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR commitment function, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the step of claim 25.

37. A method as recited in Claim 25, wherein the TCR function is a basic cryptographic primitive.

38. A method as recited in Claim 37, wherein the cryptographic primitive is the SHA-1 compress function.

39. A method as recited in Claim 26, wherein said resulting hash value is 80 bits long.

40. A method as recited in Claim 25, wherein the TCR function is a TCR hash tree based on a basic cryptographic primitive.

41. A method as recited in Claim 35, further comprising employing the TCR commitment scheme in an enhanced commitment based signature scheme.

42. A method as recited in Claim 35, further comprising employing the TCR commitment scheme in an E-commerce protocol.

43. An article of manufacture as recited in claim 42, wherein the step of generating the TCR commitment function includes:

receiving a data string to be committed and receiving secret information if any in said regular commitment scheme;

computing a regular commitment message using said regular commitment scheme upon both said data string and said secret information;

randomly selecting a key for said TCR function;

computing said TCR function on said key and said regular committment message and obtaining a resulting hash value;

forming a TCR commitment message including said resulting hash value and said key, said TCR commitment

message being an output of said TCR commitment function.

44. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for generating a TCR de-commitment function, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 29.